Notice of Allowability	Application No.	Applicant(s)	
	10/005,105	KOCHER ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to _____.

2. ☒ The allowed claim(s) is/are *1-19*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AT

DETAILED ACTION

1. Claims 1-19 have been examined.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

In the Specification:

Page 1, line 4, delete "1999" and replace with --1999, now U.S. patent 6,327,661--.

Page 1, line 11, delete "2000" and replace with --2000, now U.S. patent 6,381,699--.

Page 6, line 30, delete "1999" and replace with --1999, now U.S. patent 6,327,661--.

Page 7, line 6, delete "2000" and replace with --2000, now U.S. patent 6,381,699--.

Priority

3. Acknowledgment is made that the instant application is a continuation-in-part of Application No. 09/326,222, filed 06/03/1999, now U.S. Patent No. 6,327,661 B1, which claims priority from Provisional Application No. 60/087,880, filed 06/03/1998.

4. Acknowledgment is made that the instant application is a continuation-in-part of Application No. 09/930,836, filed 08/15/2001, now U.S. Patent No. 6,327,661 B1, which is a

continuation of Application No. 09/324,798, filed 06/03/1999, now U.S. Patent No. 6,278,783 B1 which claims priority from Provisional Application No. 60/087,826, filed 06/03/1998.

5. Acknowledgment is made that the instant application is a continuation-in-part of Application No. 09/737,182, filed 12/13/2000, now U.S. Patent No. 6,381,699 B1, which is a division of Application No. 09/224,682, filed 12/31/1998, now U.S. Patent No. 6,304,658 B1 which claims priority from Provisional Application No. 60/089,529, filed 06/15/1998 and Provisional Application No. 60/070,344, filed 01/02/1998.

Information Disclosure Statement

6. The information disclosure statements (IDSes) submitted on 08/01/2005, 06/05/2005, 05/03/2005, 01/05/2005, 12/27/2004, 11/08/2004, 09/24/2004, and 01/31/2002 were filed before the mailing date of the first Office action on the merits. The submission is in compliance with the provisions of 37 CFR 1.97(b)(3). Accordingly, the information disclosure statements are being considered by the examiner.

Allowable Subject Matter

7. Claims 1-19 are allowed.

8. The following is an examiner's statement of reasons for allowance:

9. Claims 1 and 11; 2 and 8-10; 3-7; 12-17; and 18 and 19 are drawn to three methods for evaluating the security of a cryptographic device to recover useful information about a key, a system for evaluating the security of cryptographic hardware, and a method for analyzing externally measurable characteristics of a cryptographic device, respectively. The closest prior

art, Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, and Other Systems," discloses similar methods and system. Kocher describes that, during the processing of each cryptographic operation, recording a plurality of measurements of an attribute related to the operation of a cryptographic device and statistically combing the recorded measurements (see § 6 Experimental Results, pages 107-109; figures 1 and 2; measurements of modular multiplication times and modular exponentiation times). However, he neither teaches nor suggests sending a plurality of command sequences to the device to cause the device to perform a cryptographic operation to process data using a key and determining whether information about the key is leaking from the device. These distinct steps explicitly incorporated into independent claims 1, 2, 3, 12, and 18 render claims 1 and 11; 2 and 8-10; 3-7; 12-17; and 18 and 19, respectively, allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Bennett et al., U.S. Patent No. 5,515,438 A discloses the limited ability to obtain information about the quantum key from stray light.

- Schlumberger Industries SA (Rhelimi et al.), French Patent Application Publication No. 2738970 A1 describes incorporating a cryptographic key assigned to an integrated circuit in a matrix of material with varying resistivity on the surface of the circuit
- Schlumberger Industries SA (Rhelimi et al.), French Patent Application Publication No. 2738971 A1 describes determining the key assigned to an integrated circuit stored in a matrix of material with varying resistivity by measuring voltage signals on the surface of the intergrated circuit
- Rhelimi et al., U.S. Patent No. 6,047,068 A describes a method and apparatus for determining an encryption key associated with an integrated circuit having a memory plane

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and

statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

September 30, 2005

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100